



# State of Wisconsin AND HIPAA Privacy (WorkForce)

## Health Insurance Portability and Accountability Act (HIPAA)

**Jack Hough**

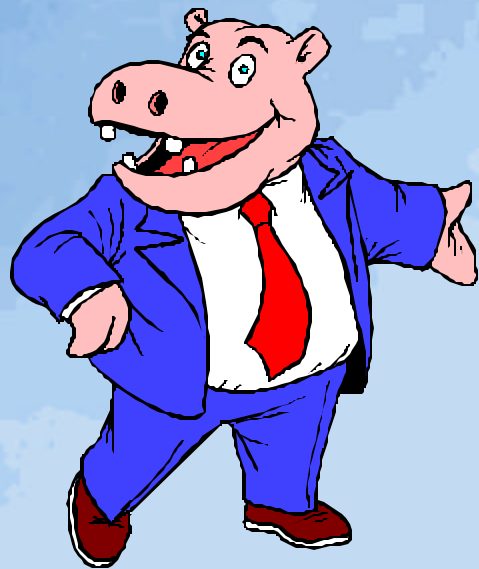


**Developed by**

**StoneHenge**  
*PARTNERS, INC.*

# HIPAA Privacy WorkForce

---



- **The Minimum Necessary Standard**
- **Privacy Training**
- **Introduction to Security**

# The Minimum Necessary Standard



- The Minimum Necessary Standard
- When Does Minimum Necessary Apply
- When Does Minimum Necessary NOT Apply
- How to Implement Minimum Necessary

# **Minimum Necessary Standard**

- The Standard:**

**Covered entity must make reasonable efforts to limit use, disclosure and requests of PHI to the minimum necessary**

- Changes from Proposed Rule**

- Exception for treatment by health care providers**
- Protocol for routine, recurring uses**
- Reasonable reliance on certain requestors**
- Justification for entire medical record**

# **Minimum Necessary Standard**

- **Reasonableness standard**
  - **Flexible—to fit own workforce/business**
  - **Scaleable**
- **How is reasonableness determined?**
  - **Healthcare size?**
  - **Content of PHI?**
  - **Prudent professional?**
  - **Best practices?**

# **Minimum Necessary Standard**

- **Consequence of violation**

- **Negligent violation - \$100-\$25,000 CMP**
- **Wrongful disclosure-criminal penalties of up to \$250,000 and 1-10 years imprisonment**
- **Common law/statutory privacy rights**

- **Recommendations**

- **Benchmark Review vs. Regulations**
- **Comparability analysis (Use of PHI)**
- **Expert opinion**

# **When Does Minimum Necessary Apply?**

- **All uses, disclosures and requests**
  - **Six (6) Exceptions**
- **For health care operations and payment purposes**
- **For treatment purposes**
  - **Exception for Providers (for treatment disclosures)**
  - **Applies to uses for treatment by providers**

# When Does Minimum Necessary Apply?

- **Business associates**
- **Disclosures Required by Law**
- **De-Identified Information**
- **Other disclosures and requests to third parties**

# When Does Minimum Necessary NOT Apply?

---

- Six (6) exceptions:

- Disclosures to and requests by providers for treatment
- Disclosures to the individual
- Disclosures authorized by the individual
- Uses and disclosures required by law
- Disclosures to HHS for Privacy Rule compliance
- Disclosures to HHS for other HIPAA compliance

# How to Implement Minimum Necessary

---

- **Define Minimum Necessary**
- **Use specifications**
- **Identify flow of PHI**
- **Define workforce Uses**
  - **Employees, volunteers, trainees, others under contracts to Covered Entities**
- **Develop policies, procedures and protocols**

# How to Implement Minimum Necessary

---

- **Determine extent of access by class**
  - Particular data elements?
  - Categorical access vs. process oriented access
- **Determine conditions to access**
- **Workforce Issues**
  - Multiple hats
  - Volunteers
  - On-site business associates
  - Overtime

# How to Implement Minimum Necessary

---

- **Disclosure/Request Specifications**
  - Standard for routine and recurring uses
- **Reasonable Restrictions for Requesting Entities**
  - Disclosure of specific data to a requesting entity
  - Public official for required reports
    - Minimum necessary representation
  - Task Force for research purposes
  - Case by Case Review for Disclosures outside defined standards.
    - **Task Force Review**
      - Disclosure criteria and procedures for reviewing requests in accordance with criteria



# Privacy Training

 **StoneHenge**  
*PARTNERS, INC.*

# Privacy Training for Employees

- **Privacy Training is one of the Top Priorities**

- **Topics for Educating the Organization:**

- **What is HIPAA?**
- **What Does HIPAA Do?**
- **Why HIPAA?**
- **How Will HIPAA Affect Us?**
- **When and What Must We Do?**
- **What are the Penalties?**

- **Privacy Training according to job function**

- **HIPAA Training must be kept current and on-going**



# Auditing of HIPAA Compliance



# Auditing of HIPAA Compliance

**All auditing and monitoring can not be addressed by technology - especially related to the privacy requirements.**

## **Manual monitoring:**

- **Review current practices vs. compliance**
- **Review forms**
- **Review system access requests (Security)**
- **Review contracts (Business Associate language)**
- **Review confidentiality statements**
- **Review Marketing materials**

# Auditing of HIPAA Compliance

- **Review Current Practices**
  - Monitor trash for disposal of PHI
  - Monitor verbal communications
  - Monitor use of screensavers
  - Monitor access to Medical Records and other PHI
  - Monitor patient care areas
  - Whiteboards

# Auditing of HIPAA Compliance

## **Technical Strategies Auditing & Monitoring**

- **Accounting of Disclosures**
  - **Trending reported complaints**
- **Monitoring minimum necessary**
- **Monitoring employee/system access**
- **Same last name monitoring**

# Auditing of HIPAA Compliance

## **Successful Approach**

- **Appointing a Privacy Officer/Privacy Manager**
- **Educating Administration and Employees**
- **Incorporating HIPAA privacy policies into existing policies**

## **Organizational Challenges**

- **Determining a reasonable approach for compliance and ongoing monitoring**
- **Ensuring that the privacy rules do not inhibit patient care**

# Introduction to Security



- Introduction to Security
- Security Relating to Privacy
- Implementation of Security Requirements



# Introduction to HIPAA Security

---

- **Technical Security Services**
  - The processes that are put in place to protect information and to control individual access to information
- **Technical Security Mechanisms**
  - Processes that are put in place to guard against unauthorized access to data that is transmitted over a communications network.
- **Electronic Signature Standard (*Optional*)**
  - A “digital signature” is an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters so that the identity of the signer and the integrity of the data can be verified.

# Introduction to HIPAA Security

---

- **What is a Contingency Plan?**
  - A plan for responding to a system emergency, that includes performing backups, preparing critical facilities that can be used to facilitate continuity of operations in the event of an emergency, and recovering from a disaster.
  - Continue critical business functions  
(*Business Continuity Plan*)
  - Retrievable exact copies of information  
(*Data backup Plan*)
  - Restore any loss of data  
(*Disaster Recovery Plan*)
  - Periodic testing  
(*Testing and Revision Procedures*)

# Introduction to HIPAA Security

---

## Privacy vs. Security

- **What is the Difference?**

- **SECURITY**

Refers to HOW private information is safeguarded—Ensuring privacy by controlling access to information and protecting it from inappropriate disclosure and accidental or intentional destruction or

- **loss  
PRIVACY**

Refers to WHAT is protected — Health information about an individual and the determination of WHO is permitted to use, disclose, or access the information

# **Security Relating to Privacy Requirements**

- **Privacy vs. Security (Examples)**

## **The Security Requirement of:**

- **Administrative Procedures**

- **Formal Mechanisms for processing records**

**Once this Security Requirement is met the following Privacy Requirements have been satisfied.**

- **Documented Processes, Policies and Procedures**

- **Physical Safeguards**

- **Assigned Security Officer**

**Once this Security Requirement is met the following Privacy Requirements have been satisfied.**

- **Assign a Security Responsibility**

# Implementation of Security Requirements

## **Security Requirements – Security vs. Privacy**

**Each Privacy requirement depends upon these Security requirements.**

- **Security Management Process**
- **Information Access Control**
- **Chain of Trust Partner Agreement**
- **Authentication**
- **Encryption**
- **Termination Procedures**
- **Training**

# Implementation of Security Requirements

## **Security Requirements – Examples (continued)**

- **Computer/Network Configuration Management**
- **Documentation**
- **Virus Checking**
- **Hardware/Software Review & Testing**
- **Inventory**
- **Security Testing**
- **Security Incident Procedures**
- **Reporting & Response**

# Implementation of Security Requirements

## **Security Requirements – Examples (continued)**

- **Internal Audits**
- **Procedures & Methodology**
- **Audit Logs**
- **Reports**
- **Automation of Programs**
- **Manual Inspections**

**For more information See the StoneHenge Booth  
or contact:  
Pat Sloan  
1-866-392-2002**



**PSLOAN@STONEHENGE.ORG  
[www.stonehenge.org](http://www.stonehenge.org)**